UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/934,166	08/20/2001	Ian Rhodes	930.337USW1	8265

32294 7590 01/12/2005

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/934,166	RHODES, IAN	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/09/2004 (amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56 and 59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56 and 59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-23 and 25-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson (US 5,548, 649), and further in view of Boyle et al (US 5,940,591).

a. *Referring to claims 1, 27, 37:*

i. Jacobson teaches:

(1) selectively routing a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route said communication according to said information held in said storage means **[i.e., referring to Figure 1, the foregoing problems are solved by a network local security bridge and corresponding method for bridging a first side of a network and a second side of the network. The first side includes local secure zone host devices within a local secure zone established by the network local security bridge. The second side includes remote secure zone host devices within remote secure zones established by network remote security bridges, wherein the bridges route the data packet from one side of the network to another (column 1, lines 27-35)]**; and

(2) encrypting said selectively routed communication by means of an encryption engine before it traverses said intermediate network, wherein said at least one network element and said encryption engine are located substantially within said first secure network **[i.e., the data packet processor encrypts the data**

frame of the first side data packet when its source and destination addresses respectively specify one of the local secure zone host devices and one of the remote secure zone host devices (column 1, lines 47-51)].

ii. Although Jacobson does not explicitly point out the distribution and/or routing of security information between the first network and the second network, Boyle teaches:

(1) Referring to Figure 2, a variation is shown employing SNIUs for internetwork connections. A bridge SNIU is used between two private networks (shaded ovals) using the same security labeling semantics but which operate at two different protection levels. The networks may be controlled by a single network security manager SM, or each network can have its own security manager SM. A gateway SNIU is used between two networks using different security labeling semantics, for example, a Type A network may use labels (Top Secret, Secret, Confidential, Unclassified) and a Type B network may use the labels (Most Secret, Secret, Restricted, Confidential, Releasable). A guard SNIU is used to support communications between a private network and a public network. The network security system of the invention is divided into two major functional areas: the Trusted Session Protocol (TSP) hosted by the SNIU, which is responsible for the management of the data path and the passing of data; and the Security Management architecture, consisting principally of the Security Manager (SM), which is responsible for security management of the network **(column 4, lines 51-67 through column 5, lines 1-4).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such distribution of security information between first network and second network in Jacobson for providing security and multi-level security for a non-secure network **(column 1, lines 13-14 of Boyle).**

iv. The ordinary skilled person would have been motivated to:

(1) include such distribution of security information between first network and second network in Jacobson since it would be highly desirable to provide multi-level security in a non-secure environment, i.e.. where both the network and the

hosts are not trusted, so that existing hosts and network assets would not have to be replaced by trusted hosts or secure network assets. It is also required that such an MLS system must provide user accountability and data integrity during all phases of operation within the network **(column 2, lines 35-41 of Boyle).**

b. *Referring to claim 2:*

i. Jacobson further teaches:

(1) wherein said at least one network element comprises switch means provided with control means and said storage means **[i.e., referring to Figure 1, network security bridges (104-1, 104-3), that are switches for "providing with control means and storage means", includes first and second side interface controllers and routes data packet from one side to another (column 1, lines 35-36)].**

c. *Referring to claims 3 and 4:*

i. Jacobson further teaches:

(1) wherein said storage means is operable to store said information comprising routing information and security information **[i.e., referring to Figure 1, the network local security bridge includes first and second side interface controllers and data packet processor for encrypting/decrypting data frame. The first side interface controller receives from the first side of the network a first side data packet and the second side interface controller receives from the second side of the network a second side data packet. The received first and second side data packets each contain a source address, a destination address, and a data frame (column 1, lines 35-43)].**

d. *Referring to claims 5-7, 14-15, 28-35, 43-46:*

i. These claims have limitations that is similar to those of claims 2-4, thus they are rejected with the same rationale applied against claims 2-4 above.

e. *Referring to claim 8:*

i. Jacobson further teaches:

(1) identifying said predetermined type of communication by means of at least one of the following: originating subscriber characteristics; destination subscriber characteristics; payload characteristics; and network service characteristics **[i.e., in the network, normal data and bridge management communication is made between and among the hosts, bridges, and the gateway with ethernet data packets (wherein "originating subscriber characteristics; destination subscriber characteristics; destination subscriber characteristics; payload characteristics; and network service characteristics" are considered to include in these data packets). These data packets include an ethernet header and an ethernet data frame. The ethernet header includes an ethernet source address, an ethernet destination address, and an ethernet protocol identifier. The ethernet data frame includes an IP header and an IP data frame or portion. The IP header includes an IP source address, an IP destination address, and an IP protocol identifier. The IP data frame includes the data that is to be communicated (column 2, lines 57-67)]**.

f. *Referring to claims 9 and 10:*

i. These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

g. *Referring to claims 11, 18-21, 36, 48-52:*

i. These claims have limitations that is similar to those of claims 1 and 4, thus they are rejected with the same rationale applied against claims 1 and 4 above.

h. *Referring to claims 12 and 13:*

i. These claims have limitations that is similar to those of claims 3 and 4, thus they are rejected with the same rationale applied against claims 3 and 4 above.

i. *Referring to claim 16:*

i. Jacobson further teaches:

(1) further comprising providing a service management access point for accessing and changing said information held in the storage means

[i.e., from the information provided by the commands, that is "for accessing and changing information held in the storage means", issued with the user terminal, the bridge manager determines that the user seeks to perform a bridge local install or view operation. After determining this, the bridge manager determines whether the user is authorized to perform the bridge local install or view operation. This is done by comparing the user's i.d. and password for accessing local bridge 104-1 with those stored in the authorization table 244 and looking up the user's authorization level in the authorization table 244 (column 10, lines 19-28)].

j. *Referring to claim 17:*

i. Jacobson further teaches:

(1) wherein said security information comprises decryption information, a distribution of said decryption information being triggered according to a predetermined schedule **[i.e., the bridges 104-1 to 104-3 include encryption and decryption software and/or hardware so that normal data communication and bridge management communication between secure zones 108-1 to 108-3 is made by encrypting and decrypting the IP data frame in the transmitted or received data packet (column 3, lines 31-36)].**

k. *Referring to claim 22:*

i. Jacobson further teaches:

(1) wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route operated by trusted network operators **[i.e., referring to Figure 1, encrypted data packets transmit through network security bridges, 104-1 to 104-3, which includes first and second side interface controllers and data packet processor for encrypting/decrypting data frame (column 3, lines 31-36)].**

l. *Referring to claim 23:*

i. Jacobson further teaches:

(1) wherein said security information is transferred to the at least one network element located in the second secure network by means of a

secure communication route over said relatively insecure intermediate network **[i.e., referring to Figure 1, encrypted data packets transmit between secure zone 108-1 to 108-3 through network security bridges, 104-1 to 104-3, and pass over the area that are not within a secure zone, which contains unsecure hosts, 102-8 to 102-10 (column 3, lines 50-67 through column 4, lines 1-7)].**

m. *Referring to claim 25:*

i. Jacobson teaches:

(1) A method for the distribution of security information between a first node and at least one second node, including the step of providing at least one network element operable to store security information and triggerable to distribute the security information from said first node to at least one node **[i.e., referring to Figure 1, network security bridges (104-1, 104-3) includes first and second side interface controllers and routes data packet from one side to another (column 1, lines 35-36)].**

ii. Although Jacobson does not explicitly point out the distribution and/or routing of security information between the first network and the second network, Boyle teaches:

(1) Referring to Figure 2, a variation is shown employing SNIUs for internetwork connections. A bridge SNIU is used between two private networks (shaded ovals) using the same security labeling semantics but which operate at two different protection levels. The networks may be controlled by a single network security manager SM, or each network can have its own security manager SM. A gateway SNIU is used between two networks using different security labeling semantics, for example, a Type A network may use labels (Top Secret, Secret, Confidential, Unclassified) and a Type B network may use the labels (Most Secret, Secret, Restricted, Confidential, Releasable). A guard SNIU is used to support communications between a private network and a public network. The network security system of the invention is divided into two major functional areas: the Trusted Session Protocol (TSP) hosted by the SNIU, which is responsible for the management of the data path and the passing of data; and the Security Management architecture,

consisting principally of the Security Manager (SM), which is responsible for security management of the network **(column 4, lines 51-67 through column 5, lines 1-4).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such distribution of security information between first network and second network in Jacobson for providing security and multi-level security for a non-secure network **(column 1, lines 13-14 of Boyle).**

iv. The ordinary skilled person would have been motivated to:

(1) include such distribution of security information between first network and second network in Jacobson since it would be highly desirable to provide multi-level security in a non-secure environment, i.e.. where both the network and the hosts are not trusted, so that existing hosts and network assets would not have to be replaced by trusted hosts or secure network assets. It is also required that such an MLS system must provide user accountability and data integrity during all phases of operation within the network **(column 2, lines 35-41 of Boyle).**

n. *Referring to claim 26:*

i. Jacobson teaches:

(1) A method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, including the step of providing at least one network element operable to store security information and triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network. **[i.e., referring to Figure 1, the network local security bridge includes first and second side interface controllers and data packet processor for encrypting/decrypting data frame. The first side interface controller receives from the first side of the network a first side data packet and the second side interface controller receives from the second side of the network a second side data packet. The received first and second side data**

packets each contain a source address, a destination address, and a data frame (column 1, lines 35-43). In addition, the data packet processor encrypts the data frame of the first side data packet when its source and destination addresses respectively specify one of the local secure zone host devices and one of the remote secure zone host devices (column 1, lines 47-51)].

ii. Although Jacobson does not explicitly point out the distribution and/or routing of security information between the first network and the second network, Boyle teaches:

(1) Referring to Figure 2, a variation is shown employing SNIUs for internetwork connections. A bridge SNIU is used between two private networks (shaded ovals) using the same security labeling semantics but which operate at two different protection levels. The networks may be controlled by a single network security manager SM, or each network can have its own security manager SM. A gateway SNIU is used between two networks using different security labeling semantics, for example, a Type A network may use labels (Top Secret, Secret, Confidential, Unclassified) and a Type B network may use the labels (Most Secret, Secret, Restricted, Confidential, Releasable). A guard SNIU is used to support communications between a private network and a public network. The network security system of the invention is divided into two major functional areas: the Trusted Session Protocol (TSP) hosted by the SNIU, which is responsible for the management of the data path and the passing of data; and the Security Management architecture, consisting principally of the Security Manager (SM), which is responsible for security management of the network **(column 4, lines 51-67 through column 5, lines 1-4).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such distribution of security information between first network and second network in Jacobson for providing security and multi-level security for a non-secure network **(column 1, lines 13-14 of Boyle).**

iv. The ordinary skilled person would have been motivated to:

(1) include such distribution of security information between first network and second network in Jacobson since it would be highly desirable to provide multi-level security in a non-secure environment, i.e.. where both the network and the hosts are not trusted, so that existing hosts and network assets would not have to be replaced by trusted hosts or secure network assets. It is also required that such an MLS system must provide user accountability and data integrity during all phases of operation within the network **(column 2, lines 35-41 of Boyle).**

o. *Referring to claims 41, 42, 55:*

i. These claims have limitations that is similar to those of claims 25-26, thus they are rejected with the same rationale applied against claims 25-26 above.

p. *Referring to claims 38, 39:*

i. Jacobson further teaches:

(1) including decryption means located substantially within the second secure network; wherein said decryption means are provided at the second end terminal **[i.e., referring to Figure 1, the data packet processor, which includes in network security bridge, decrypts the data frame of the second side data packet when its source and destination addresses respectively specify one of the remote secure zone host devices and one of the local secure zone host devices (column 1, lines 55-59)].**

q. *Referring to claim 40:*

i. Jacobson further teaches:

(1) wherein said decryption means are provided at a node other than the second end terminal **[i.e., referring to Figure 1, network security bridges (104-1 to 104-3) includes data packet processors, these are "decryption", for decrypting the data frame. Jacobson discloses three different data packet processors as shown in Figure 1].**

r. *Referring to claim 47:*

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

s. *Referring to claim 53:*

i. This claim has limitations that is similar to those of claim 22, thus it is rejected with the same rationale applied against claim 22 above.

t. *Referring to claim 54:*

i. This claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

u. *Referring to claim 56:*

i. This claim has limitations that is similar to those of claims 1 and 26, thus it is rejected with the same rationale applied against claims 1 and 26 above.

3. Claims 24 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson, and further in view of Thomas (US 6,421, 339 B1).

a. *Referring to claims 24 and 59:*

i. Jacobson does not mention:

(1) providing said routing and/or access point to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network.

ii. Thomas teaches:

(1) allowing a H.323 compliant user to roam to another H.323 compliant network that is recognized by that users home gatekeeper. After arriving at the visited network, the roaming user registers with a visited gatekeeper. The visited gatekeeper authorizes the registration by determining the network of the roaming user and that a roaming agreement exists between the visited and home network **(column 6, lines 20-27).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such roaming agreement in Jacobson's network security bridging system to have a capability to call to a H.323 compliant data packet network **(column 6, lines 40-42 of Thomas).**

iv. The ordinary skilled person would have been motivated to:

(1) include such roaming agreement in Jacobson's network security bridging system for accommodating roaming endpoint users across H.323 compliant network domains **(column 1, lines 6-8 of Thomas).**

Response to Argument

3. Applicant's arguments filed August 9, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

Jacobson fails to disclose or suggest this feature and merely describes transmitting encrypted and decrypted packets from one node to another within a network. Jacobson does not disclose or suggest distributing the secured information that is used for encrypting and decrypting the packets.

Examiner maintains that:

Jacobson does teach the claimed subject matter. Furthermore, turning back to Figures 2 and 4a-4c, if the identification table does contain the parsed IP source address, this means that the received data packet is from one of the remote secure zones and its IP data frame has been encrypted by the corresponding network remote security bridge. By this point, the data packet forwarder will have already determined that the received data packet has an IP destination address that specifies one of the local secure zone hosts 102-1 or 102-2 (decision block 432 of Figure 4b). As a result, the data packet forwarder selects a source key from the key table 232 in the library 216 for decrypting the IP data frame of the received data packet (block 436 of Figure 4b) (column 7, lines 34-45).

Applicant further argues that:

Jacobson does not disclose or suggest distributing security information to certain target nodes that provide at least one network element operable to store security information and triggerable to distribute the security information from the first node to at least one target node. Thus, Jacobson does not disclose or suggest at least these features of the pending claims.

Examiner still maintains that:

Jacobsom teaches the claimed subject matter. Referring again to Figures 2 and 4a-4c, the data packet forwarder 211 selects the source key by first identifying from the identification table 230 the IP address of the network remote security bridge that establishes the remote secure zone which contains the remote secure zone host specified by the parsed IP source address. Then, it selects the source key in the key table 232 that corresponds to the network remote security bridge that it just identified. After the source key has been selected, the data packet forwarder calls up the encryptor/decryptor 233 and passes to it the pointer to the received data packet. The encryptor/decryptor in response decrypts the IP data frame of the received data packet with the selected source key using the DES table 234 contained in the library 216 in accordance with known DES encryption/decryption techniques (block 438 of Figure 4b). The encryptor/decryptor then alerts the data packet forwarder that the IP data frame of the received data packet has been decrypted. The data packet forwarder then returns control to the operating system 210, alerts the operating system that the received data packet has been processed and is to be forwarded to the side opposite from where it was received, and also passes to the operating system the pointer to the received data packet (block 408 of Figure 4c) (column 7, lines 54-67 through column 8, lines 1-10). Since independent claims 41-42, 55-56 have limitations that is similar to those of claims 25-26, therefore, the same rejection is still maintain for these independent claims.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date

of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
January 6, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21[illegible]